Smart Card Specification
Manufacturer - Matrix Research Limited
Product Brand - ACX

1. Smart Card

a) The smartcard shall be based on international standards, complying with ISO/IEC 14443-2/3 A for contactless communications. The smart card security shall be EAL5+ security certified. This Subcontractor shall submit the details for review without objection by the Architect and Engineer before implementation.
b) The Smart Card memory is 4K bytes of memory
c) The smartcard shall be designed to securely read, interpret, and authenticate access control data using 13.56 MHz contactless smartcard credentials.
d) This subcontractor shall provide an Encoder for card programming with 128-bit AES and/or 3K3AES encryption and a site-specific key. The operator shall keep the card key. This Subcontractor shall provide the Operator all necessary software, tools, and training for keeping the card key.
e) The Smart Card for the Access Control System shall use MIFARE DESFire EV3 technology and card format. The encryption method shall be 128-bit AES and/or 3K3DES, subject to the approval of the f Architect and/or Engineer.
f) The Smart Card shall be protected against card cloning. All card data and keys shall be encoded and encrypted by 128-bit AES and/or 3K3AES.
g) Card Serial Number (CSN) without encryption protection shall not be used to identify the smart card.
h) The Smart Card offers contactless read-and-write smartcard technology and anti-counterfeiting features, including direct custom color artwork or photo identification.
i) The smartcard shall be of laminated plastic, factory-coded with a combination of facility codes and an individual identification number included in the encoded information. They shall be durable and difficult to duplicate without the facilities used in manufacturing. Any attempt to reach wires embedded in the cards shall destroy the card.
j) Badge and credit-sized cards shall be suitable for being laminated with a barcode label and a badge ID, which includes a color photograph of the authorized holder.
k) The card skins shall be labeled according to the requirements of the Architect but shall not extend beyond placing a colored graphic logo, name, return address, and the ID mentioned.
l) The system shall include all color-printing artwork on the smart card.
m) Their operation shall not be affected by metallic coins, mechanical keys, or other electronic card keys, nor shall they affect bank credit cards in a wallet. They shall also be immune to external magnetic fields and RF interference.
n) The contactless smart card shall meet the following material and construction specifications:

i. PVC card materials.
ii. The card surface shall be glossy and made of a material compatible with direct-to-card dye-sublimation or thermal transfer printing.
iii. Card construction shall meet durability requirements and size (53.98mm × 85.60mm × 0.76mm) according to ISO 7810.
iv. The internal antenna configuration shall allow a single slot punch on the vertical (short) side of the card.
v. The card may be marked with an external ID number in inkjet or laser-etched numbering and shall match the internally programmed ID number. If the external number does not match the internal number, a cross-reference list is provided to detail the internal/external numbering sequences